DPSN International Data Protection Day work-in-progress event on Friday 27th January 2023 online

The Data Protection Law Scholars Network

Stream 1!

Data Protection Law Scholars Network

Frederik Zuiderveen Borgesius

Prof ICT & Law

iHub

Radboud University

Research themes

- Interdisciplinary research
- Data protection & privacy
- Non-discrimination

PhD candidates

Predictive policing:

- Ruben te Molder
- Pieke de Beus

AI & discrimination:

- Marvin van Bekkum
- Tim de Jonge

Impact of AI on autonomy:

- Shima Abbady

Cyber Security:

- Mattis van ’t Schip

DPSN International Researchers Online Meet-up

DATA GOVERNANCE AND AI

Lawfulness of personal data processing for AI development

VRIJE
UNIVERSITEIT
BRUSSEL

Pablo Trigo Kramcsák
PhD researcher
Research Group on Law, Science,
Technology & Society (LSTS), VUB

LSTS

DATA PROCESSING AS A CORE ASPECT FOR DEVELOPING AI/ML MODELS

DATA CURATION FOR AI

- Expansion of AI systems. Improvement of computer processing capacities: data-driven society.
- The precision and effectiveness of AI models are highly dependent on the availability of genuine, relevant, and representative training data. Trustworthy AI with reliable outputs.
- At all steps of AI design and development, different types of personal data processing operations can take place.
- Data curation is a fundamental aspect of the "AI data governance framework", geared to generating appropriate procedures that guarantee the availability, labeling, and use of high-quality data.
- Challenges:
    - Practical difficulties: costs; limited benchmark databases.
    - Regulatory challenges, especially visible in the personal data protection field.

DATA PROCESSING IN AI CONTEXTS

TENSION WITH DATA PROTECTION LAW PRINCIPLES

- Collection limitation, purpose specification, and use limitation; data minimization; transparency; data quality, access, and correction; retention limitation; automated decision-making and profiling.
- Certain collective dimensions or effects of such data processing operations should also be kept in mind.
- One of the main difficulties that arise in data processing for AI development relates to the lawful collection and processing of databases that serve for AI design, training, and testing
- Although there is no hierarchy among the different legal bases for data processing, in doubtful cases, consent is generally understood by data controllers as a preferred or default choice for lawful data processing.
- Difficulties: to collect multiple consents from different data subjects; to ensure that these indications comply with the validity criteria settled out in the data protection regulation.
- The prominent role of consent as a legal ground for processing personal data is questioned: it is not inherently better or more important than other lawful bases, as it would not necessarily constitute evidence of real protection of personal data.

THE ROLE OF THE LEGITIMATE INTEREST

CAN AI DEVELOPERS RELY ON THE LEGITIMATE INTEREST LAWFUL BASIS?

- Legitimate interest (LI) as an appropriate legal ground for processing personal data to train a machine learning model (ICO, AEPD).
- LI: interest of data controller (AI developer) or third parties (including the interest of society as a whole o certain groups that may be affected by possible algorithmic biases).
- LI rests on a system of balance between different interests and conflicting rights. Legitimate Interests Assessment (balancing test).
- It must not be understood as a soft option for AI developers.
- Special attention should be given to additional safeguards aimed at protecting the interests or rights and freedoms of data subjects (e.g., anonymization/deidentification techniques, strong pseudonymization practices, "synthetic data", and privacy-enhancing technologies)
- It is particularly important to determine the potentially harmful impact of a given AI system, as well as its purposes.

中国政法大学
CHINA UNIVERSITY OF POLITICAL SCIENCE AND LAW

Lost in Translation

How co-regulatory tools excluded self-regulation in China's privacy governance

Zeng Chen
China's University of Political Science and Law
The Institute of Administrative Law
2222010042@cupl.edu.cn
2023.01.27

Prepared solely for Data Protection Law Scholars Network International Researchers Online Meet-up Event
Please do not circulation with the athor's permission

Case of technical standards

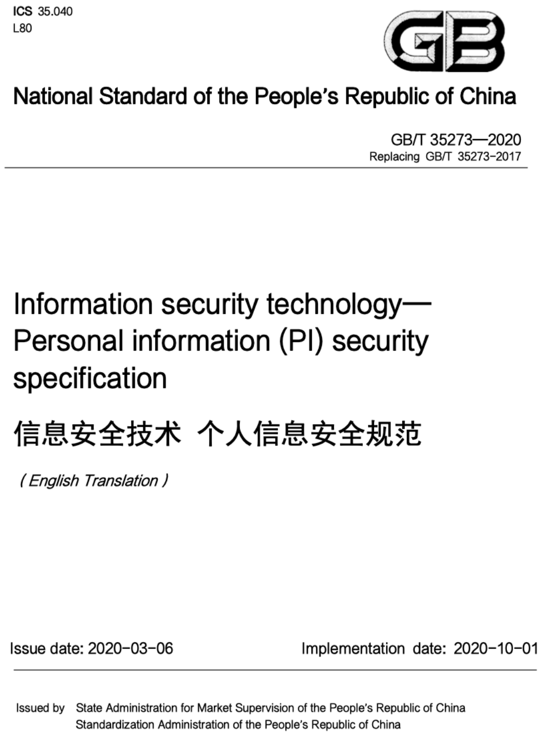
Self-regulation under the shadown of CAC in China’s tech industry

Promise：
-promoting the collaboration between government and indusrty

Reality:
-technical standards act as explanatory tools of principle-based legislation

- Hardening
- Obscuring
- Overstepping

Consequences:
-reinforce CAC’s regulatory power
without the limitations of due process
nor the rule of law



ICS 35.040
L80

GB

National Standard of the People’s Republic of China

GB/T 35273—2020
Replacing GB/T 35273–2017

Information security technology—
Personal information (PI) security
specification

信息安全技术 个人信息安全规范

(English Translation)

Issue date: 2020-03-06 Implementation date: 2020-10-01

Issued by State Administration for Market Supervision of the People’s Republic of China
Standardization Administration of the People’s Republic of China

中国通信标准化协会
China Communications Standards Association

TAF
taf.org.cn taf.net.cn

TC 全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

Bibliography

- Grafenstein, Maximilian. "Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the'State of the Art'of Data Protection-by-Design." *Forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics,* Edward Elgar Publishing (2019).

- Kamara, Irene. "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation'mandate'." European journal of law and technology 8.1 (2017).

- Ponte, Stefano, Peter Gibbon, and Jakob Vestergaard. Governing through standards: Origins, drivers and limitations. Palgrave Macmillan, 2011.

- Gutwirth, Serge, et al., eds. Reinventing data protection?. Springer Science & Business Media, 2009.

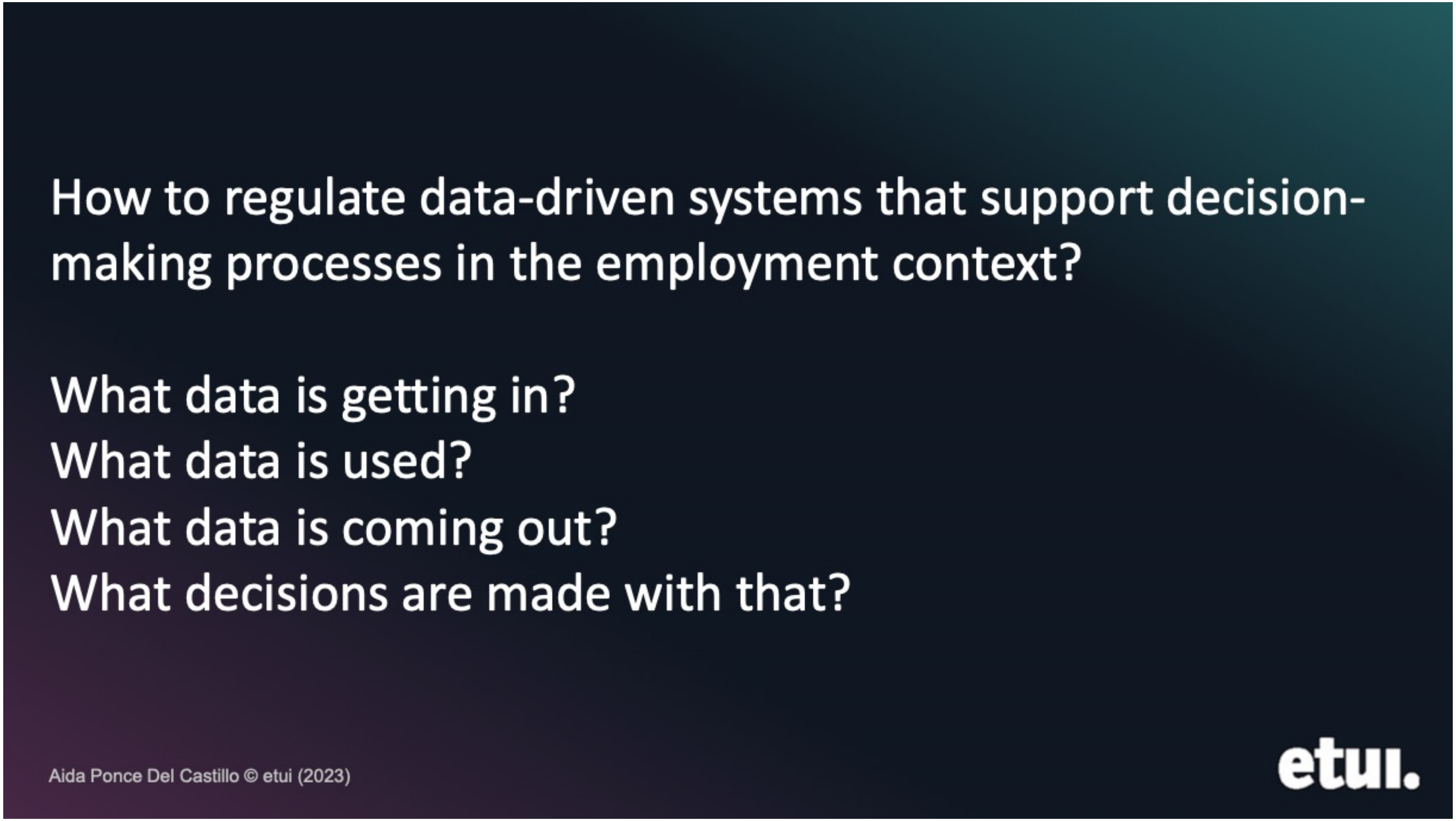
Prepared solely for Data Protection Law Scholars Network International Researchers Online Meet-up Event
Please do not circulation with the athor's permission

International Data Protection Day
Data Protection Law Scholars
NetworkJanuary 27 2022, online

Data Protection in the context of employment

Aida Ponce Del Castillo, ETUI
Senior researcher
Foresight Unit
European Trade Union Institute, Brussels

etui.

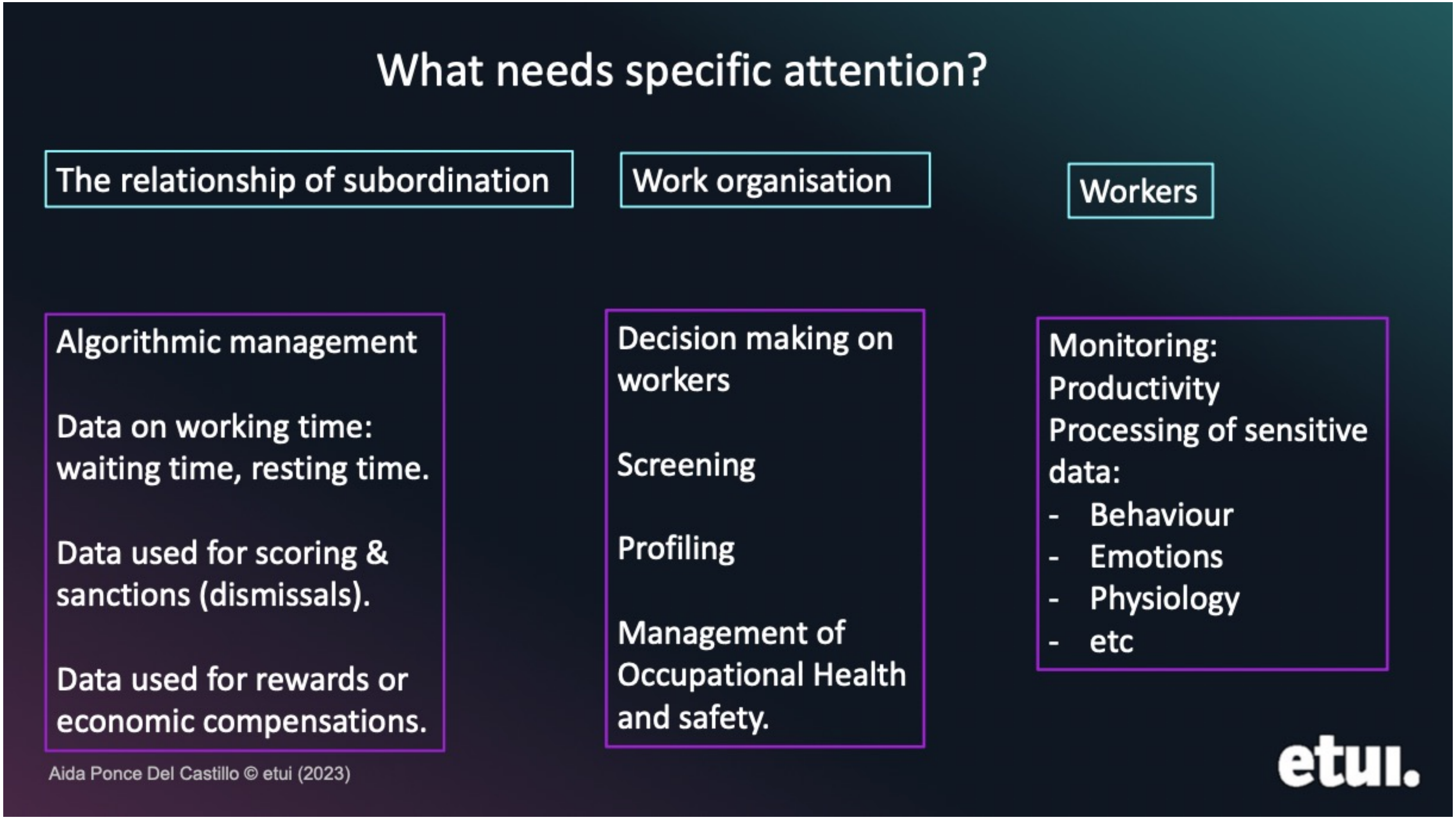


How to regulate data-driven systems that support decision-making processes in the employment context?

What data is getting in?
What data is used?
What data is coming out?
What decisions are made with that?

etui.

GDPR provisions apply in the context of employment, but they might require some adaptations in order to provide genuine protection to workers.



What needs specific attention?

The relationship of subordination

Algorithmic management

Data on working time: waiting time, resting time.

Data used for scoring & sanctions (dismissals).

Data used for rewards or economic compensations.

Work organisation

Decision making on workers

Screening

Profiling

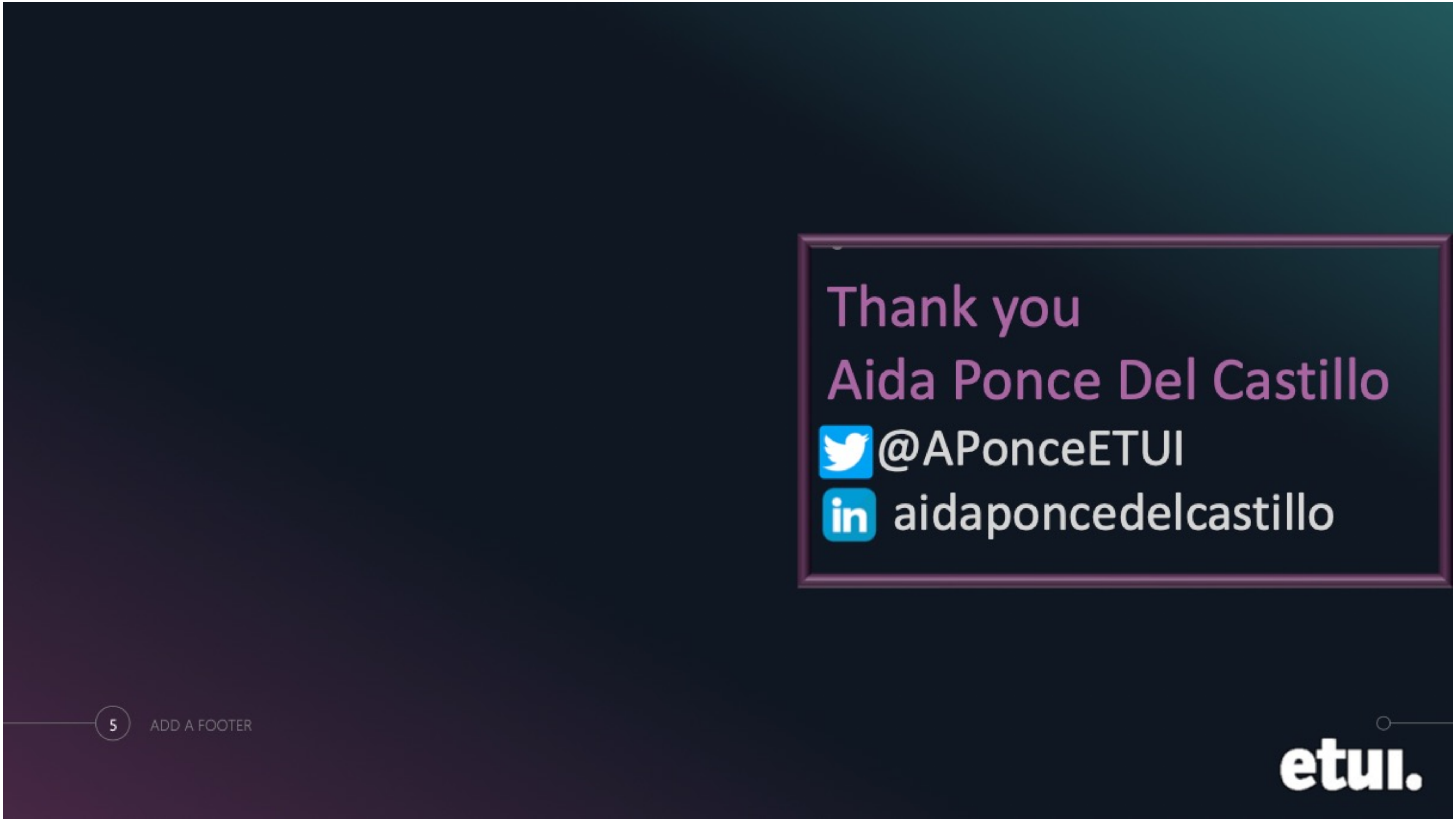
Management of Occupational Health and safety.

Workers

Monitoring:
Productivity
Processing of sensitive data:

- Behaviour
- Emotions
- Physiology
- etc

Aida Ponce Del Castillo © etui (2023)



Thank you

Aida Ponce Del Castillo

@APonceETUI

aidaponcedelcastillo

UVA DATA SCIENCE

Jess Reia [they/them], Assistant Professor of Data Science

Addressing Data Protection for Gender-Diverse Communities across the Americas

January 27, 2023 | reia@virginia.edu | @jhereia | @jessreia@mastodon.social

Overview

- Who: Transgender communities (trans, gender non-conforming, nonbinary, Two-spirit)
- Problem: Data collection of gender-diverse individuals allows us to think about the benefits and risks of (in)visibility
- Invisibility in data policy for evidence-based policymaking
- Visibility sheds light on issues around privacy and data protection
- Regions: Brazil and the United States

Small and big data collection

Census

Health, education, and social welfare records

Community-based counting

Research projects

Regulatory frameworks and other guidances

Transnational

Federal
State
Local

Research ethics boards

Codes designed by communities

How to get involved

Urban Data Equity Lab

Workshops

Interviews and focus groups

Smart mobility and dumb data law

Dr. Gerard J. Ritsema van Eck
@Gerard_RvE
mstdn.social/@Gerard
g.j.ritsema.van.eck@step-rug.nl

Province: autonomous vehicles

KPN: Data ownership

A Taxonomy of Privacy Enhancing Functionalities

Kartik Chawla (Tilburg University)

A Taxonomy of Privacy Enhancing Functionalities

- Kartik Chawla | PhD Candidate | TiSEM, PBLL, JADS

- In interacting with website ToSs, users interact with ***digitally intermediated standard form contracts***, i.e., ‘Digital Standard Agreements’.
- Not a smart contract *per se*, but works similar to imperative smart contracts.
- Three categories of contractual ‘Tasks’.

Category	User Goals
Negotiation	[G1] Make an informed choice about how their personal data will be processed.
Monitoring	[G2] Identify breaches of their preferences by the publisher if they occur.
Dispute/ Terminate	[G3] Enforce or terminate the agreement.

Hurdles to the performance of Tasks

Category	Control Tasks	Hurdles
Negotiation	[Tn1] Read documentation and cookie notice.	1. [N1] Ex-ante Information Asymmetry a. [N1.1] Behavioural biases b. [N1.2]Long/complex documentation 2. [N2] Ex-ante Transaction Costs a. [N2.1] Granularity problem 3. [N3] Opportunism (Dark patterns) a. [N3.1] Negotiation power imbalance
	[Tn2] Select appropriate cookie agreement.	
	[Tn3] Store agreement communicated and documentation for future reference.	
	[Tn4] Modify agreement if necessary.	
	[Tn5] Repeat Tn1-3 in case of modification of documentation or notices by Publisher.	
Monitoring	[Tm1] Monitor compliance with agreement directly.	1. [M1] Ex-post monitoring costs a. [M1.1] Lack of auditing tools and methods 2. [M2] Opportunism (Monitoring) a. [M2.1] Insufficient monitoring
	[Tm2] Monitor compliance with agreement indirectly.	
Dispute/ Terminate	[Td1] Enforce agreement via direct interaction with the publisher.	1. [DT1] Ex-post information asymmetry 2. [DT2] Insufficient enforcement a. [DT2.1] DPA enforcement issues b. [DT2.2] Ex-post enforcement costs
	[Td2] Enforce terms via third party, including judicial enforcement.	
	[Td3] Implement technical controls.	
	[Td4] Withdraw consent or terminate agreement.	

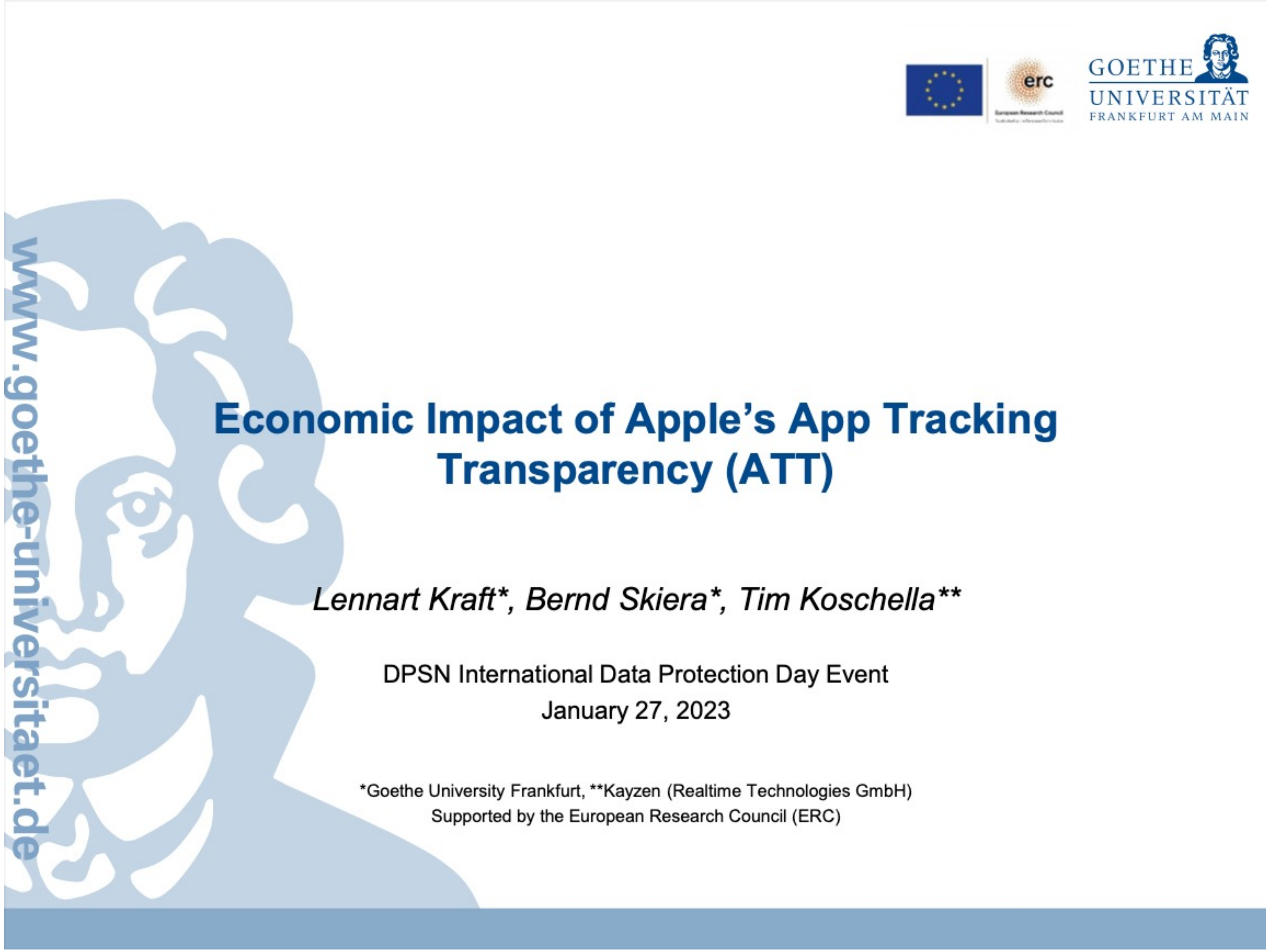
The PEF Taxonomy

- 5 Meta-Dimensions:
  - Domain & User Interface
  - Negotiation, Monitoring, Enforcement
- 17 dimensions
- 65 functionalities
- Sample:
  - Consent-O-Matic

MD1 Domain	D1 Preference Representation	Publisher's ToS		Public Law (aka default rules)		Industry Standard	Custom
	D2 Interoperability	Indifferent		Cooperative		Adversarial	
MD2 User Interface	D3 Timing	At Setup	Just-in-Time	Context-dependent	Periodic	Peripheral	On Demand
	D4 Channel	Primary		Secondary		Public	
	D5 Modality	Visual		Auditory		Haptic	
	D6 Control	Blocking		Non-Blocking		Decoupled	

MD3 Negotiation

D7 Transparency	D8 Communication of Acceptance	D9 Granularity of Acceptance	D10 Consent Storage	D11 Modification
Translation	Automated Selection	Accept/Reject/Manage	Local	Allow User Modification
Summarisation		More information		
Chunking	Non-ToS User Preferences	Vendor-based choices		
Visualisation				
Interaction	Opt-in	Purpose-based choices	Non-Local	Notify User of Modified Terms
Customisation				
Third-party links	Opt-out	Sliding Scale		
Comparison				



Economic Impact of Apple's App Tracking Transparency (ATT)

Lennart Kraft, Bernd Skiera*, Tim Koschella***

*Goethe University Frankfurt, **Kayzen (Realtime Technologies GmbH)

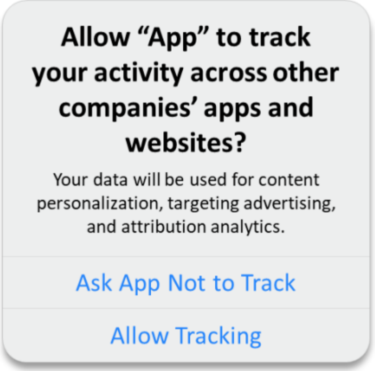
DPSN International Data Protection Day Event
January 27, 2023

Supported by the European Research Council (ERC)

Importance of Tracking via Advertiser Identifiers on Apple Devices

- **Identifier for Advertisers (IDFA)**
  - Description
    - Identifier of Apple devices
    - Enables to track users within and across apps
  - Importance
    - Advertisers' ability to target and measure ad performance
    - Publishers' ability to earn advertising revenue

- **App Tracking Transparency (ATT)**
  - Apple's new privacy framework (via iOS 14.5, on April 26, 2021)
  - Publishers require customers' (explicit) consent to use IDFA for tracking (i.e., opt-in approach)
  - Customers can more easily deny tracking

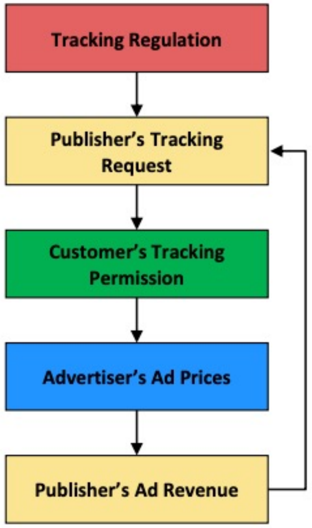


Allow "App" to track your activity across other companies' apps and websites?

Your data will be used for content personalization, targeting advertising, and attribution analytics.

Impact of ATT on Online Ad Market

Value Chain of Apple's Mobile Ad Market



Tracking Regulation

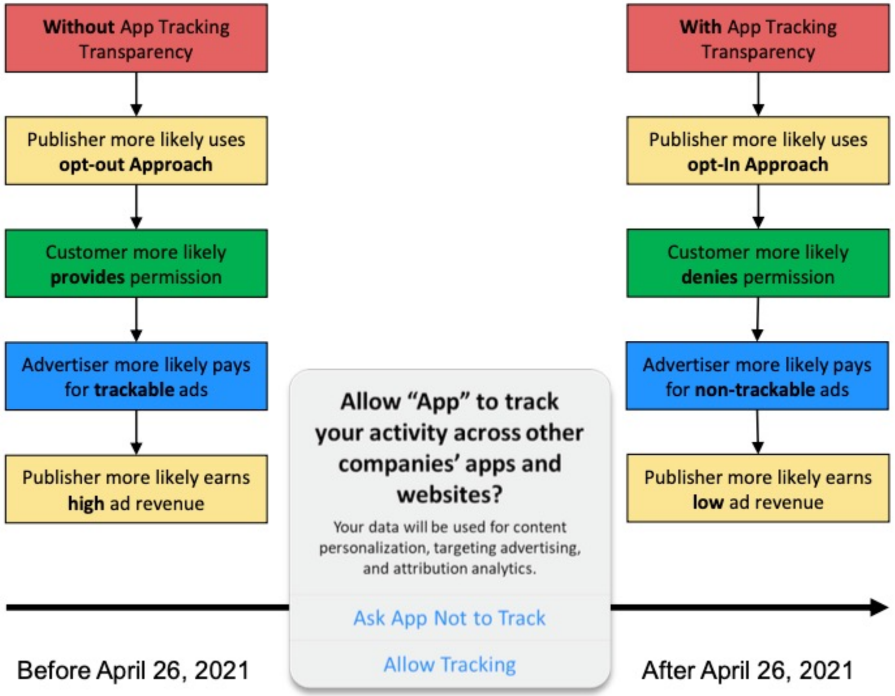
Publisher's Tracking Request

Customer's Tracking Permission

Advertiser's Ad Prices

Publisher's Ad Revenue

Hypothesized Impact of ATT on Value Chain



Without App Tracking Transparency

Publisher more likely uses **opt-out Approach**

Customer more likely **provides** permission

Advertiser more likely pays for **trackable** ads

Publisher more likely earns **high** ad revenue

With App Tracking Transparency

Publisher more likely uses **opt-In Approach**

Customer more likely **denies** permission

Advertiser more likely pays for **non-trackable** ads

Publisher more likely earns **low** ad revenue

Allow "App" to track your activity across other companies' apps and websites?

Your data will be used for content personalization, targeting advertising, and attribution analytics.

Ask App Not to Track

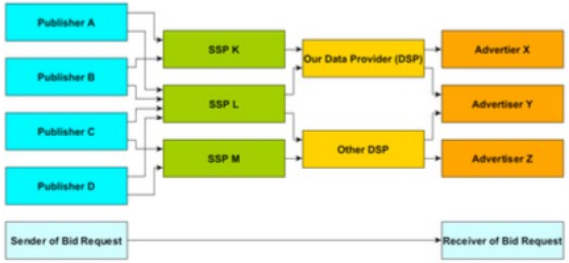
Allow Tracking

Before April 26, 2021

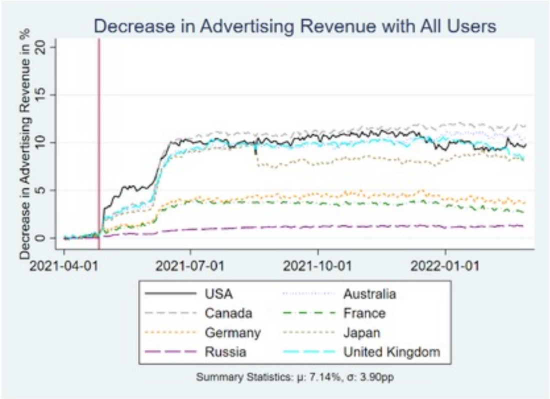
After April 26, 2021

Summary of Empirical Study

- **Description of Data Provider and Dataset**
  - DSP for >50bn daily RTB mobile bid requests
  - Scope of dataset
    - EU (e.g., GER) and Non-EU countries (e.g., USA)
    - Apr. 1, 2021 – Feb. 28, 2022



- **ATT's Economic Impact (USA)**
  - 69.68% decrease in IDFA availability
  - 19.20% decrease in ad revenue with Apple users
  - 9.82% decrease in ad revenue with all users



Summary Statistics: μ: 7.14%, σ: 3.90pp

- **Conclusions and Implications**
  - Economic impact of opt-out vs. opt-in approach
  - Lower profitability of tracking-based apps
    - Apps serving ads
    - Apps collecting and selling data
  - Substantial differences across countries

Note: DSP: Demand-Side-Platform, RTB: Real-Time-Bidding

Thank You For Your Attention!

Lennart Kraft
lennart.kraft@wiwi.uni-frankfurt.de

Bernd Skiera
skiera@wiwi.uni-frankfurt.de

Tim Koschella

Protect

Towards a duty of assistance to improve transparency practices

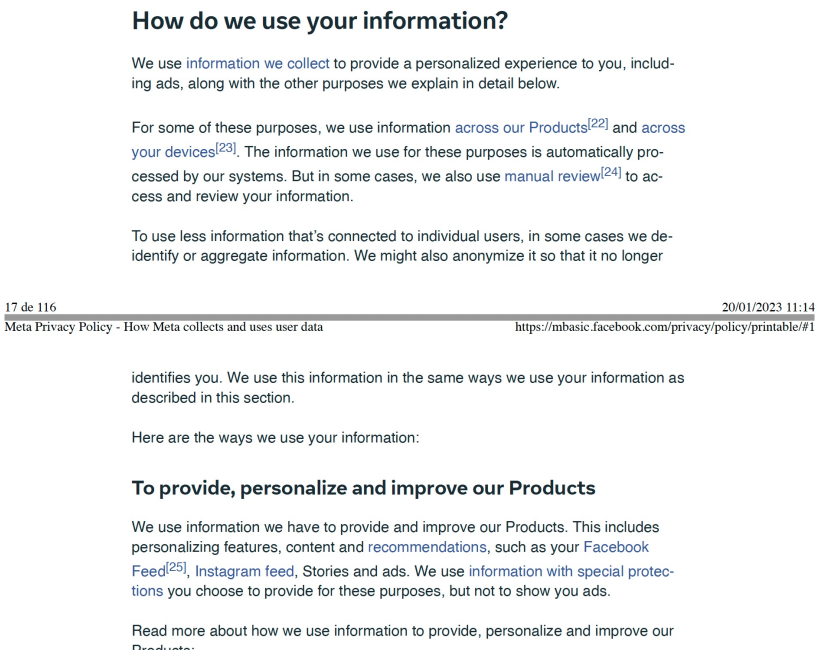
Andrés Chomczyk, VUB – LSTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 813497.

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

Assisting the data subject: learning from financial services

Meta's current privacy notice (20/01/2023)



How do we use your information?

We use information we collect to provide a personalized experience to you, including ads, along with the other purposes we explain in detail below.

For some of these purposes, we use information across our Products[22] and across your devices[23]. The information we use for these purposes is automatically processed by our systems. But in some cases, we also use manual review[24] to access and review your information.

To use less information that's connected to individual users, in some cases we de-identify or aggregate information. We might also anonymize it so that it no longer

17 de 116 20/01/2023 11:14

Meta Privacy Policy - How Meta collects and uses user data https://mbasic.facebook.com/privacy/policy/printable/#1

identifies you. We use this information in the same ways we use your information as described in this section.

Here are the ways we use your information:

To provide, personalize and improve our Products

We use information we have to provide and improve our Products. This includes personalizing features, content and recommendations, such as your Facebook Feed[25], Instagram feed, Stories and ads. We use information with special protections you choose to provide for these purposes, but not to show you ads.

Read more about how we use information to provide, personalize and improve our Products:

https://mbasic.facebook.com/privacy/policy/printable/#1

Meta's last notes exchange tender offer (29/11/2022)

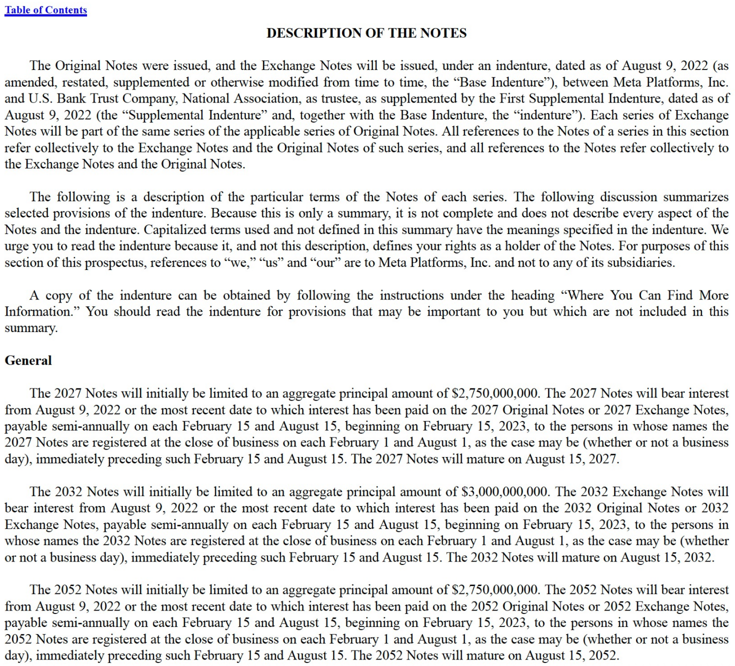


Table of Contents

DESCRIPTION OF THE NOTES

The Original Notes were issued, and the Exchange Notes will be issued, under an indenture, dated as of August 9, 2022 (as amended, restated, supplemented or otherwise modified from time to time, the "Base Indenture"), between Meta Platforms, Inc. and U.S. Bank Trust Company, National Association, as trustee, as supplemented by the First Supplemental Indenture, dated as of August 9, 2022 (the "Supplemental Indenture" and, together with the Base Indenture, the "indenture"). Each series of Exchange Notes will be part of the same series of the applicable series of Original Notes. All references to the Notes of a series in this section refer collectively to the Exchange Notes and the Original Notes of such series, and all references to the Notes refer collectively to the Exchange Notes and the Original Notes.

The following is a description of the particular terms of the Notes of each series. The following discussion summarizes selected provisions of the indenture. Because this is only a summary, it is not complete and does not describe every aspect of the Notes and the indenture. Capitalized terms used and not defined in this summary have the meanings specified in the indenture. We urge you to read the indenture because it, and not this description, defines your rights as a holder of the Notes. For purposes of this section of this prospectus, references to "we," "us" and "our" are to Meta Platforms, Inc. and not to any of its subsidiaries.

A copy of the indenture can be obtained by following the instructions under the heading "Where You Can Find More Information." You should read the indenture for provisions that may be important to you but which are not included in this summary.

General

The 2027 Notes will initially be limited to an aggregate principal amount of $2,750,000,000. The 2027 Notes will bear interest from August 9, 2022 or the most recent date to which interest has been paid on the 2027 Original Notes or 2027 Exchange Notes, payable semi-annually on each February 15 and August 15, beginning on February 15, 2023, to the persons in whose names the 2027 Notes are registered at the close of business on each February 1 and August 1, as the case may be (whether or not a business day), immediately preceding such February 15 and August 15. The 2027 Notes will mature on August 15, 2027.

The 2032 Notes will initially be limited to an aggregate principal amount of $3,000,000,000. The 2032 Exchange Notes will bear interest from August 9, 2022 or the most recent date to which interest has been paid on the 2032 Original Notes or 2032 Exchange Notes, payable semi-annually on each February 15 and August 15, beginning on February 15, 2023, to the persons in whose names the 2032 Notes are registered at the close of business on each February 1 and August 1, as the case may be (whether or not a business day), immediately preceding such February 15 and August 15. The 2032 Notes will mature on August 15, 2032.

The 2052 Notes will initially be limited to an aggregate principal amount of $2,750,000,000. The 2052 Notes will bear interest from August 9, 2022 or the most recent date to which interest has been paid on the 2052 Original Notes or 2052 Exchange Notes, payable semi-annually on each February 15 and August 15, beginning on February 15, 2023, to the persons in whose names the 2052 Notes are registered at the close of business on each February 1 and August 1, as the case may be (whether or not a business day), immediately preceding such February 15 and August 15. The 2052 Notes will mature on August 15, 2052.

https://www.sec.gov/Archives/edgar/data/1326801/000095010322020353/dp184651_424b3.htm

Ensuring adequate information for the data subject?

Consent's role in the EU's Data Strategy

Privacy notices are here to stay… so how can we make them useful?

Critical issues

Third parties or data controllers?

Can this advice be trusted?

Does this advice qualify as a nudge and compromise consent?

Sito web DECEPTICON:
https://irisc-lab.uni.lu/deceptive-patterns-online-decepticon-2021-24/
shorturl.at/hsHK4

Fonds National de la Recherche Luxembourg

DECEPTICON: Fighting back dark patterns with interdisciplinary powers

Arianna Rossi

SnT, Université du Luxembourg

DPSN International Data Protection Day – 27.01.23

UNIVERSITY OF LUXEMBOURG

Bongard et al., 2021. ***I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous! - Dark Patterns from the End-User Perspective.*** **DIS ACM pp. 763-776**

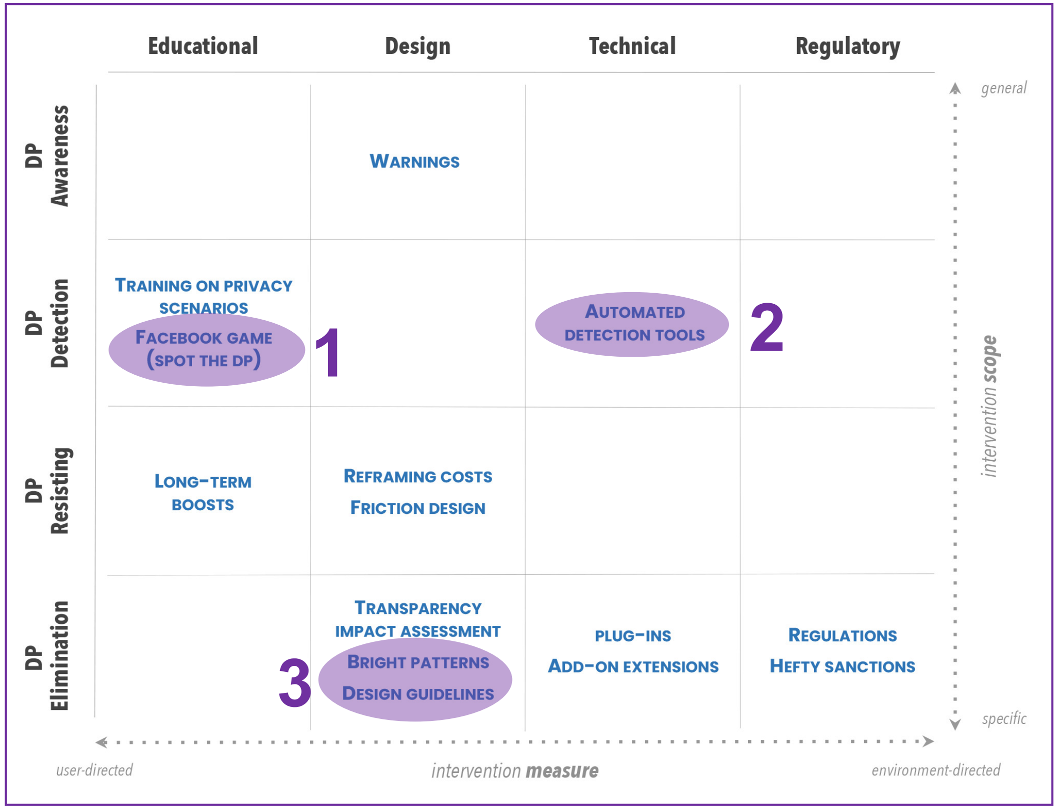
Why do dark patterns work and how should we fight them?

Results:

- **Awareness is not enough**
- **Older than 40, less educated** users are more vulnerable
- Those who can detect dark patterns declare to **resist their influence** more
- Dark patterns are everywhere, we should **report them and eliminate them** from the web

Thus:

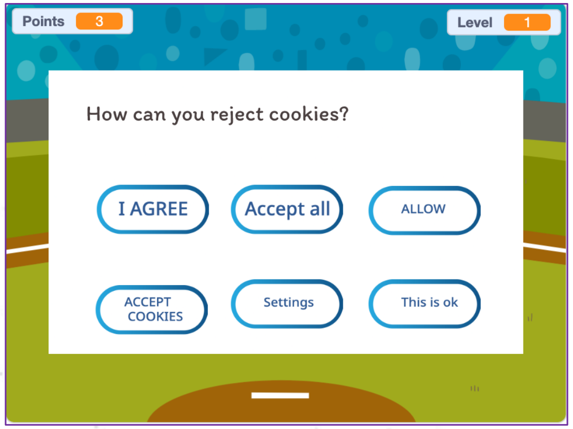
1. How might we bolster users' capacity to recognize and respond to dark patterns?
2. How might we scale up our capacity to detect dark patterns?
3. How might we provide actional guidance to companies to avoid dark patterns and implement legal design patterns?



	Educational	Design	Technical	Regulatory
DP Awareness		Warnings		
DP Detection	Training on privacy scenarios Facebook game (spot the DP)		Automated detection tools	
DP Resisting	Long-term boosts	Reframing costs Friction design		
DP Elimination		Transparency impact assessment Bright patterns Design guidelines	Plug-ins Add-on extensions	Regulations Hefty sanctions

3 types of interventions to 1. bolster resistance; 2. scale up detection; 3. implment legal design patterns

1. «Dark cookie» game



How can you reject cookies?

- **Discover and learn to respond** to dark patterns
- Goal: **reject all non-essential cookies**
- Open source - Scratch
- **Game design patterns** for others to adopt and implement

2. MISP crowdsourcing

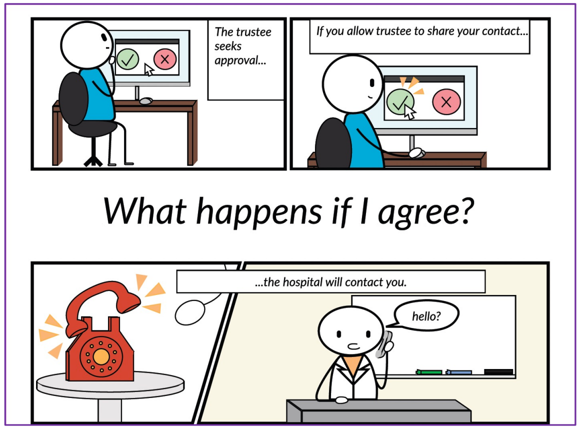
UNIVERSITÉ DU LUXEMBOURG

MISP Threat Sharing

Welcome to the Dark Patterns MISP community hosted by the IRiSC Research Group at SnT, uni.lu

- **Crowdsourcing** of dark patterns on social media
- **MISP open-source platform** to share knowledge
- **Dark pattern ontology** (harms, legal requirements and their violations, etc.)

3. Legal design patterns



The trustee seeks approval...
If you allow trustee to share your contact...
What happens if I agree?
...the hospital will contact you.
hello?

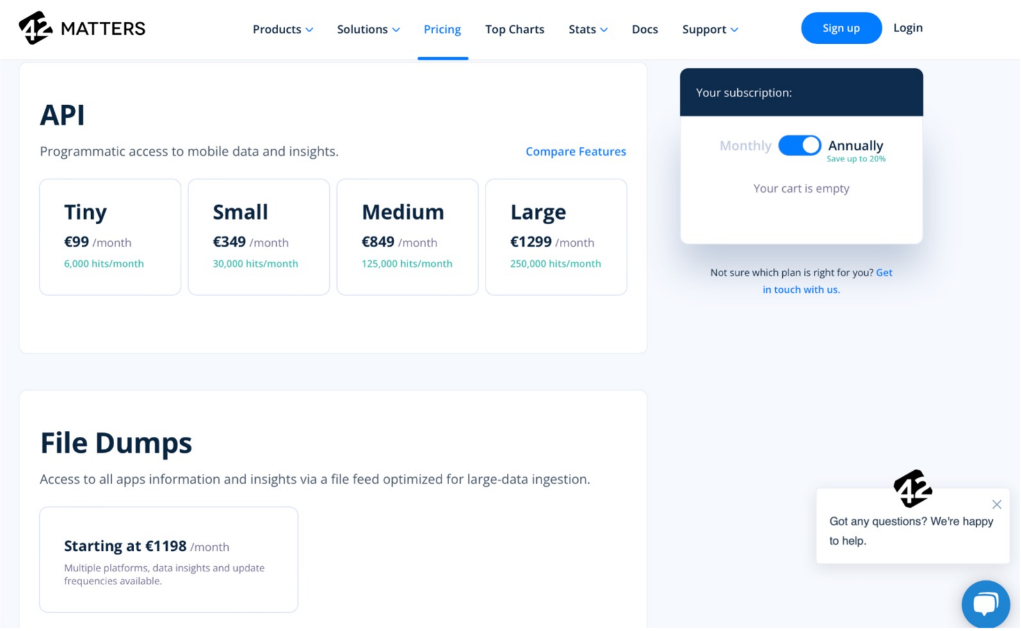
- **Transparency-enhancing p.**
- **Consent** in data spaces **(DGA)**
- **Various mediums** (e.g., comics, infographics, videos, ..)
- For **various audience** types vs 1 standard
- Effects of **framing**

Ready for the EU Digital Services Act?

How Decisions by Apple and by Google impede App Privacy

UNIVERSITY OF OXFORD
DEPARTMENT OF COMPUTER SCIENCE

UKRI Engineering and Physical Sciences Research Council



API

Programmatic access to mobile data and insights.

Compare Features

Tiny	Small	Medium	Large
€99 /month	€349 /month	€849 /month	€1299 /month
6,000 hits/month	30,000 hits/month	125,000 hits/month	250,000 hits/month

Your subscription:

Monthly ● Annually
Save up to 20%

Your cart is empty

Not sure which plan is right for you? Get in touch with us.

File Dumps

Access to all apps information and insights via a file feed optimized for large-data ingestion.

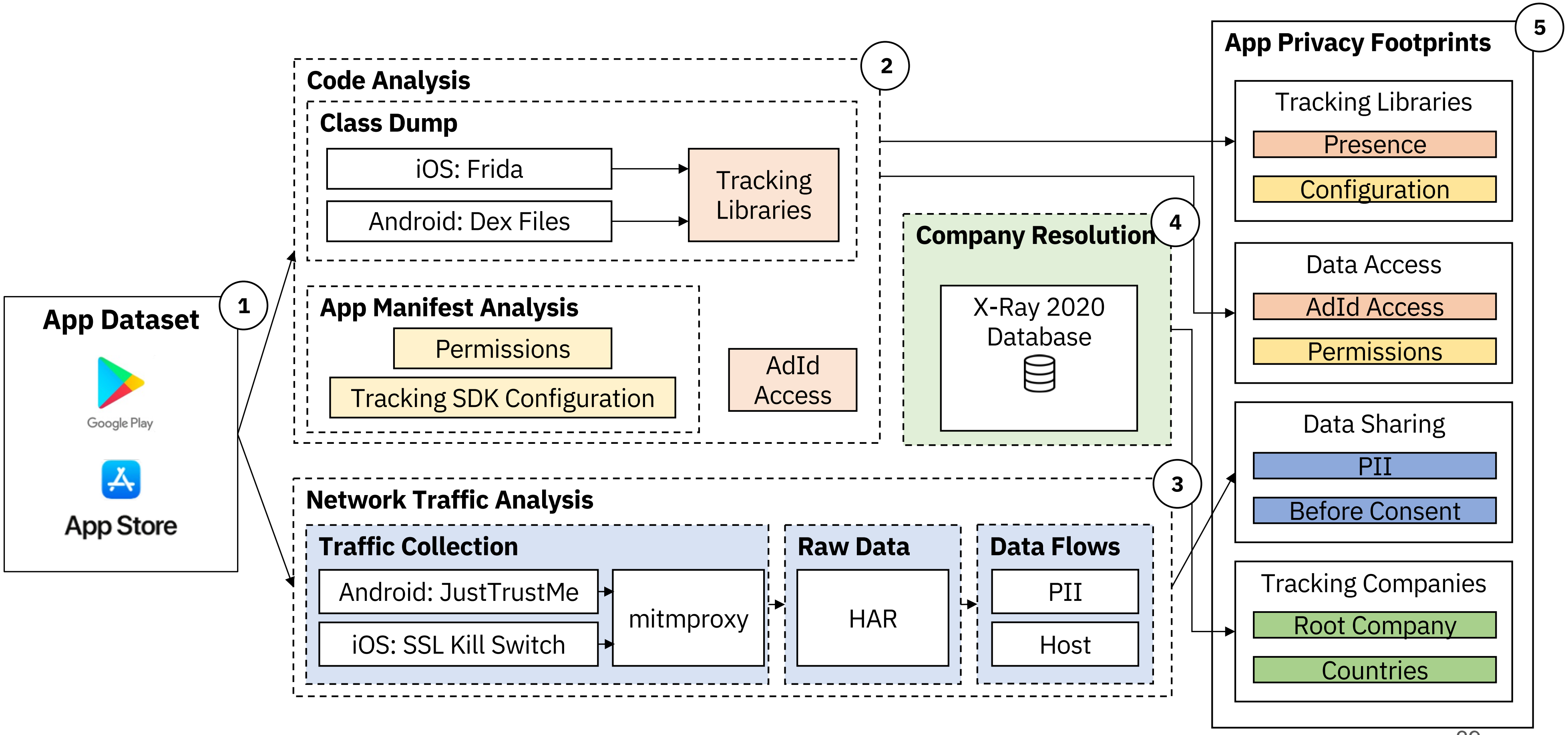
Starting at €1198 /month
Multiple platforms, data insights and update frequencies available.

Got any questions? We're happy to help.

2nd DPSN Data Protection Day, 27th of January 2023

Konrad Kollnig

PlatformControl
Privacy analysis of iOS and Android apps at scale



All code at https://www.platformcontrol.org/

- Download of App Packages and Information
    - Lack of public APIs and restrictions on scraping
    - Limited insights into app ranks, installs and permissions on iOS
    - Misleading privacy labels
    - No reporting of third-party libraries
    - Difficulty of downloading apps
    - Encryption of *all* iOS apps and paid Android apps
- Data Analysis
    - Use of closed-source and proprietary technologies
    - Google “Privacy” Sandbox for Android
    - Obfuscation of apps
    - De-facto ban of self-signed certificates on Android
    - Restrictions on system modification
- Platform Conduct
    - No programmes for academic researchers
    - Lack of engagement with GDPR requests
    - Bans of privacy software on app stores
    - Lack of compliance guidance
    - Contractual obligations on researchers